UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,265	12/28/2001	Koichi Ito	1573.1010	2775

21171 7590 05/16/2006

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
SZYMANSKI, THOMAS M	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/028,265	ITO ET AL.	
	Examiner	Art Unit	
	Thomas Szymanski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,8,9,16,18-21,25 and 29-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *4,8,9,32-41,50-57 and 64-71* is/are allowed.

6)☒ Claim(s) *1,3,16,18-21,25,29-31,42-49 and 58-63,72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3-4, 8-9, 16, 18-21, 25, and 29-72 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 25 and 72 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims refer to a "program stored on a storage medium" wherein a storage medium has not been defined as being a computer or machine readable storage medium it is non-statutory. The simple inclusion of computer or machine in reference to the type of storage medium would make such a claim statutory. The use of the term device has been taken to refer directly to an invention realized as a machine as cited in the provided definition thus making the claimed invention statutory in reference to the other claims, however, as stated previous when claiming a storage medium it must be recited as being machine or computer readable.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 3, 16, 18-20, 21, 25, 29-31, 42-49, and 58-63 are rejected under 35 U.S.C. 102(b) as being anticipated by Kawamura et al European Patent Application EP 0981223 A2.

6. Regarding Claim 1: q fixed values, where q is an integer equal to two (paragraph 0010, Fig 4) two tables of mask values are provided.

A selector for selecting one of q said fixed values in response to a randomly generated number (paragraph 0009, 0043-0044, Fig 4)

XORing an input with an XOR of a key with said selected fixed value (Fig 2, Fig 4, paragraph 0026-0029) As stated the input values are XORed with the randomly selected pattern.

The number of sets of tables is q=2, and $C_{0,j}$ Xor $C_{1,j}$ = $(10101010)_2$ or $(01010101)_2$, $D_{0,j}$ Xor $D_{1,j}$ = $(10101010)_2$ or $(01010101)_2$, is satisfied, where a fixed table before masking is defined as S[x], and j-th masked table is defined as $S_j[x \text{ XOR } C_{i,j}] \text{ XOR } d_{i,j}$ (j = 0, 1, ...15) (Fig 1, 4, 10, paragraph 0026-0044, 49-50, 55) As shown within the figure there are exactly two separate possibilities for tables. Additionally, the values are satisfied for conditions in the circuit where a specific value of the given table may be xored to satisfy the above given equation as it relates to masking/unmasking of the data bits.

$FM_{o,h} = C_h \text{ XOR } L1_0(FMin)$, $C_h = C_{h,15}\, C_{h,1} \ldots C_{h,0}$, and $D_h = dh_{,15} d_{h14} \ldots d_{h,0}$ are satisfied (Fig 4-5, Paragraphs 38-52) As provided in the reference the mask is selected in accordance with the prior art specified conditions which provide for values that anticipate the above equation.

Linear transform means L1 and L2, nonlinear transform means s[x] operate in the ith round (Fig 1-2, 4, 10, 11, 13, 16, 22, paragraphs 19-47) Per the permutation as given within the figures it can be clearly seen that such transformation take place as a process of each round.

Second selector for selecting one of q sets of masked fixed tables in response to a random number. Nonlinear transforming an input in accordance with the selected set of fixed tables (Fig 4, paragraph 0026-0030) The transform takes place as a function of the inverse of p. This provides for the stated nonlinear transformation.

7. Regarding Claim 3: encrypting unit comprising first XOR and nonlinear transform means (Fig 1, 2, 4, paragraph 0009, 0022, 0029)

Second XOR means for XORing an input to the encryption unit with a fixed value selected in response to the random number (Fig 4)

Third XOR means for XORing an output of the encryption unit with the fixed value selected in response to the random number (Fig 4) The system as denoted within figure 4 provides for a means of XORing the input, and output, as well as performing the nonlinear transform as described previously all within the scope of XORing the necessary values to obtain the intermediate masked values.

8. Regarding Claim 16: each of a plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto (Fig 1-2, paragraph 0019-0023) Each iteration provides for the necessary components.

9. Regarding Claim 18: Plurality of encrypting rounds (Fig 1, paragraph 0019-0024)

Fixed tables for the plurality of respective rounds are identical (Fig 1, Fig 4) As shown once a random value indicates the table for performing that particular mask function it does not change over the permutations.

10. Regarding Claim 19: a mask is cancelled over subsequent ones of the rounds (Fig 19-22) As is the purpose of the invention the mask must be cancelled or removed before the value can be passed on and used for its originally intended purpose.

11. Regarding Claim 20: masking is performed in each of a second plurality of encrypting rounds of said first plurality of encrypting rounds, said second plurality being smaller that the first plurality (Fig 1, paragraph 0020) As stated the successive rounds of the permutation occur on subsets of the data and are therefore smaller.

12. Regarding Claims 29-31: Linear transform means L1(x)=x L2(x)= Shift(x), L2(x)= MixedColumn(shift(x)) (Fig 1-2, 4, 10, 11, 13, 16, 22, paragraphs 19-47) The manner of performing a permutation upon the data as required by the specific encryption/decryption algorithm inherently provides for the use of linear transforms such as though disclosed by the applicant.

13. Claims 21, 25, 42-49, and 58-63 are merely recitations of claims 1, 3, 16, 18-20 and 29-31 in variant forms and as such are rejected on the same basis.

Response to Arguments

14. Applicant's arguments filed 2/21/2006 have been fully considered but they are not persuasive. As admitted to by the applicant in the reply on pages 18 – 19: "Kawamura describes switching between two sets of fixed mask values and tables for

each process in accordance with a random number. ... Since Kawamura describes switching between two sets of fixed mask values and tables for each process in accordance with a random number, and the two sets are complements of each other in terms of bits, Kawamura corresponds to the case in the present application in which the number of sets is limited to q=2."

15. The reference of Kawamura thus anticipates the claim language as stated wherein q=2.

16. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., providing higher security than 2^{23} steps for DPA) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

17. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

18. The arguments provided in relation to $FM_{0,h}$ and C_h, $C_{0,j}$ Xor $C_{1,j} = (10101010)_2$ or $(01010101)_2$, $D_{0,j}$ Xor $D_{1,j} = (10101010)_2$ or $(01010101)_2$, and do not specifically point out how they differentiate from the Kawamura reference. The reference of Kawamura indicates various viable bit patterns that may be used for masks as outlined in the above rejection. These values under conditions of the circuit may satisfy such an equation.

19. Kawamura in accordance with the process of encryption/decryption and as seen from the rejection presented above provides for linear transform means as specified by the applicant.

Allowable Subject Matter

20. Claims 4, 8-9, 32-41, 50-57, and 64-71 are allowed.

21. The following is a statement of reasons for the indication of allowable subject matter: As indicated by the applicant on pages 18-20 of the response the system of Kawamura does not indicate the usage of 3 or more sets of masks, but instead indicates two sets of masks, which are complements of each other. The prior art cited does not indicate any tendency for the use of more than two sets of masks and thus the applicants invention in relation to claims 4, 8-9, 32-41, 50-57, and 64-72 are allowable.

22. Claim 72 would be allowable if rewritten or amended to overcome the rejection(s) under 35 USC § 101, set forth in this Office action.

Conclusion

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

25. Inquiries concerning this communication or earlier communications from the examiner should be directed to Thomas M. Szymanski who can be reached at (571) 272-8574. The examiner's normal working schedule is between the hours 8:00am – 4:30pm (EST), Monday – Friday.

26. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

27. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).